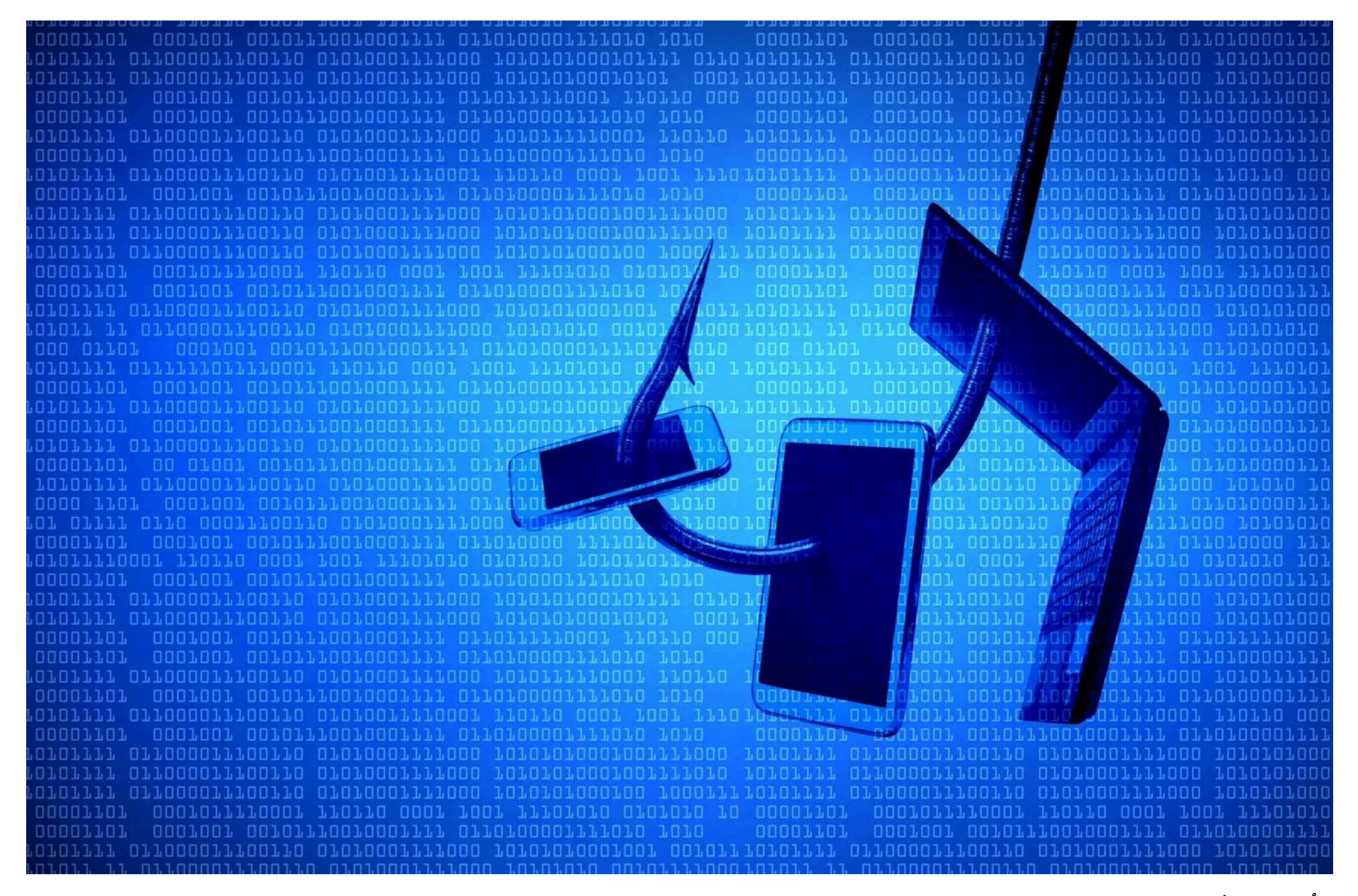
«مايكروسوفت» تتصدى لـ1.6 مليون محاولة اختراق أمني في الساعة

خوارزميات ذكية في المعركة ضد الاحتيال السيبراني



تُستخدم أدوات الذكاء الاصطناعي لإنشاء متاجر إلكترونية وهمية في دقائق ما يزيد صعوبة التمييز بينها وبين الحقيقية (شاترستوك)

لندن: نسيم رمضان

نُشر: 12:59-18 أبريل 2025 م . 20 شوّال 1446 هـ

أضحى الذكاء الاصطناعي أداةً يُحتفى بها بقدر ما يُساء استخدامها. وتسعى «مايكروسوفت» إلى تعزيز التزامها بحماية بيئتها الرقمية من خلال استراتيجية متعددة الأبعاد لمكافحة الاحتيال والانتهاكات السيبرانية. وفي تقريرها الأخير بعنوان «إشارات سيبرانية» (Cyber Signals)، كشفت الشركة عن حجم التهديدات التي واجهتها بين أبريل (نيسان) 2024 وأبريل 2025، وكذلك عن الدفاعات الواسعة التي نشرتها للتصدي لها.

خلال هذه الفترة، نجحت «مايكروسوفت» في إحباط محاولات احتيال بقيمة 4 مليارات دولار، ورفضت 49 ألف طلب شراكة احتيالي، وحجبت نحو 1.6 مليون محاولة تسجيل عبر الروبوتات في الساعة الواحدة. يركز تقرير هذا العام على كيفية تغيير الذكاء الاصطناعي طبيعة الاحتيال، ليس فقط من حيث التعقيد، بل من حيث سهولة الوصول إليه أيضاً. إذ يستخدم مجرمو الإنترنت أدوات الذكاء الاصطناعي لصناعة عمليات احتيال أكثر إقناعاً، بسرعة أكبر وبتكلفة أقل. ووفقاً لـ«مايكروسوفت»، فإن جزءاً كبيراً من هذا النشاط ينطلق من أسواق رقمية رئيسية مثل الصين وألمانيا؛ نظراً لحجم التجارة الإلكترونية فيهما.

تصاعد الاحتيال المدعوم بالذكاء الاصطناعي

أصبح الذكاء الاصطناعي يخفض الحواجز أمام الجرائم السيبرانية. فبفضل أدوات قادرة على تصفح الإنترنت لاستخلاص بيانات حساسة عن الشركات وموظفيها، يمكن للمهاجمين تصميم حملات هندسة اجتماعية معقدة. تشمل هذه الحملات مواقع تجارة إلكترونية وهمية، وشعارات مقلدة، وتقييمات مزيفة، وحتى روبوتات دعم عملاء تستند إلى الذكاء الاصطناعي قادرة على خداع المستخدمين.

كما يستغل المحتالون الذكاء الاصطناعي لإنتاج مقاطع فيديو مزيفة (Deepfakes)، واستنساخ الأصوات، وإرسال رسائل تصيُّد إلكتروني يصعب التفرقة بينها وبين الرسائل الحقيقية. تنتشر كذلك عروض وظائف مزيفة ومقابلات عمل وهمية باستخدام تقنيات توليد النصوص والصور، مستهدفة الباحثين عن العمل.



أطلقت «مايكروسوفت» سياسة جديدة تُلزم فرق التطوير بتضمين تقييمات لمخاطر الاحتيال ضمن مراحل تصميم المنتجات (شاترستوك)

الاحتيال في التجارة الإلكترونية

تشير «مايكروسوفت» إلى تصاعد إنشاء متاجر إلكترونية احتيالية في دقائق معدودة باستخدام أدوات الذكاء الاصطناعي مقارنةً بالأيام أو الأسابيع التي كانت تحتاج إليها سابقاً. تقوم هذه المتاجر بتقليد علامات تجارية معروفة، وإنتاج أوصاف وصور واقعية للمنتجات، وحتى استخدام روبوتات دردشة مدعومة بالذكاء الاصطناعي للتفاعل مع العملاء.

لمواجهة ذلك، عززت «مايكروسوفت» منتجاتها بإجراءات أمنية صارمة. على سبيل المثال، يتضمن «مايكروسوفت إيدج» (Microsoft Edge) الآن ميزة حماية من أخطاء الكتابة في عناوين المواقع، وحظر لانتحال النطاقات، بالإضافة إلى مانع صفحات التحذير الاحتيالية المبني على التعلم الآلي.

«الهندسة الاجتماعية» دون ذكاء اصطناعي

ليس كل أنواع الاحتيال تعتمد على الذكاء الاصطناعي. ففي أبريل 2024، رصدت فرق الأمان في «مايكروسوفت» نشاطاً متزايداً من مجموعة «Storm - 1811»، وهي مجموعة إجرامية مالية استغلت أداة «مايكروسوفت كويك أسست» (Windows Quick Assist). قامت المجموعة بانتحال صفة موظفي الدعم التقني واستخدمت تقنيات «التصيّد الصوتي» (vishing) لخداع الضحايا ومنحهم صلاحية الوصول عن بُعد.

أوضحت «مايكروسوفت» أن «Quick Assist» لم يتعرض للاختراق، وإنما تم استغلال وظيفته المشروعة. استجابت الشركة بإضافة رسائل تحذيرية ضمن الأداة، وتقوم الآن بحظر أكثر من 4400 محاولة اتصال مشبوهة يومياً، أي ما يعادل 5.46 في المائة من إجمالي الجلسات عالمياً.

ولتقليل المخاطر، توصي «مايكروسوفت» باستخدام أداة «ريموت هيلب» (Remote Help) للدعم التقني في المؤسسات، حيث تُستخدم داخلياً ضمن بيئة المؤسسة وتوفر مستوى أمان أعلى.

يُستخدم الذكاء الاصطناعي من قِبل المحتالين لإنشاء مواقع وهمية تقييمات مزيفة مقابلات عمل غير حقيقية ومقاطع فيديو مزيفة (شاترستوك)

تدابير على مستوى المؤسسات

تمتد بنية «مايكروسوفت» لمكافحة الاحتيال لتشمل أدوات متعددة، منها «مايكروسوفت ديفندر فور كلاود» (Microsoft Defender for Cloud) الذي يراقب موارد «أزور» (Azure) ويكشف عن الثغرات والتهديدات. كذلك «مايكروسوفت إيدج» (Microsoft Edge) الذي يحظر المواقع الاحتيالية ويكشف عن محاولات انتحال الهوية. أما البصمة الرقمية «ديجيتال فنغربرينتينغ» (Digital Fingerprinting)، فتستخدم الذكاء الاصطناعي والتعلم الآلي لرصد السلوك الاحتيالي في حين يحلل «مايكروسوفت ديفندر سمارت سكرين» (Microsoft Defender SmartScreen) سلوك المواقع وسمعتها لحظر الروابط الضارة.

من خلال تقنيات الكشف المدعومة بالذكاء الاصطناعي وإشارات الاحتيال اللحظية، تعمل «مايكروسوفت» على إيقاف البنية التحتية الخبيثة بسرعة. كما يتعاون فريق الجرائم الرقمية التابع لها مع سلطات إنفاذ القانون حول العالم لتفكيك الشبكات الإجرامية؛ ما أسفر عن مئات الاعتقالات والإجراءات القانونية.

الاحتيال في الوظائف والعروض المزيفة

يستغل المحتالون الذكاء الاصطناعي لتوليد إعلانات وظائف مزيفة وسير ذاتية ومقابلات عمل وهمية. لمكافحة ذلك؛ تنصح مايكروسوفت بتفعيل المصادقة متعددة العوامل لحسابات أصحاب العمل والتحقق من هوية أصحاب العمل عبر مواقعهم الرسمية. أيضاً توصي بالحذر من العروض التي تتطلب دفعاً أو التي تُرسل من عناوين بريدية غير موثوقة والانتباه لمؤشرات المقابلات المزيفة مثل عدم التزامن بين الصوت والصورة، أو الكلام المتقطع. وتدمج «مايكروسوفت» الوقاية من الاحتيال في عملية تطوير منتجاتها. وبدءاً من يناير (كانون الثاني) 2025، تُلزم مبادرة «Secure Future Initiative» جميع الفرق بتضمين تقييمات لمخاطر الاحتيال ضمن مراحل تصميم المنتجات.

نصائح لحماية المستهلكين

تنصح «مايكروسوفت» المستخدمين باتباع الخطوات التالية لحماية بياناتهم:

- الحذر من العروض العاجلة أو «لفترة محدودة»

- التحقق من عناوين المواقع قبل النقر على الروابط

- تجنب التحويلات البنكية المباشرة أو الدفع بالعملات الرقمية

- التأكد من مصداقية أصحاب العمل وعدم مشاركة معلومات شخصية أو مالية دون تحقق

تتطور مقاربة «مايكروسوفت» لمكافحة الاحتيال بتطور التهديدات. وفي وقت أصبح فيه الذكاء الاصطناعي سلاحاً بيد كل من المهاجمين والمدافعين، تتبنى الشركة موقفاً واضحاً، وهو تطوير منتجات مضادة للاحتيال بطبيعتها، وتزويد المستخدمين بالأدوات والمعرفة التي يحتاجون إليها للبقاء آمنين.

